STATE OF INDIANA
WEB-BASED COMPUTING GUIDELINES FOR PROSPECTIVE VENDORS

Reference:	Indiana Office of Technology (IOT) Information Technology Policy (ITP) 00-7
Technology Profile:	Applications Development
Specific Area:	Internet Portal Management
Document Type:	Architecture Guideline
Date:	July 1, 2005 (re-issued)

Purpose

This document is intended to inform prospective bidders of the state's IT architecture, including various standards and guidelines, that support our web-based computing environment.

Background

The State of Indiana built, and is committed to maintaining, a cost effective web-based computing environment. This environment is capable of supporting various web pages and applications while remaining mindful of security and privacy considerations. The overall value of users interacting with their State government as a single entity and not as a series of independent agencies and support processes is a key element of Indiana's goal to deliver government services and processes effectively to its citizens and internal departments and organizations. The State further recognizes that multiple vendors and technology platforms will be deployed to extend e-government services.

This document is intended to inform prospective bidders of the State's IT architecture, including various standards and guidelines, that support our web-based computing environment. Compliance with the standards and guidelines shall be considered when evaluating proposals for State web-based systems. In addition, this document provides general direction regarding security, common look and feel and architecture concerns for web-based pages and applications. It is targeted at all organizations, agencies, vendors and individuals developing web-based pages and applications for the State web environment to include intranet, extranet and Internet.

Those dealing with the State's architecture should employ a flexible approach. A flexible approach identifies technical areas that must conform to specific standards and allows other parameters to vendor or agency preference. While a flexible approach allows for the most competitive and open development environment, security risks can become more prevalent. Therefore, it is important to provide technical and business direction to ensure appropriate security mechanisms are implemented in information technology systems to minimize these security risks as much as possible.

There are many present demands, as well as opportunities, that State government officials are considering in order to cut costs and increase effectiveness. One method is to develop highly reusable, portable, and scalable web applications that can share access to agency data available on the State's campus backbone. Also, as State agencies rely on third party vendors for development, the State can protect its investment by ensuring that vendors develop according to the State's open architecture strategic direction. These standards will help support an agency's need to ensure the portability necessary to host their applications and pages on a variety of hardware and operating system platforms. The standards also greatly increase and ensure the compatibility, reusability, and scalability of web applications, which will improve on application performance, maintenance, and support issues. The goal of these standards and architectures is to enhance an agency's ability to shorten development time, ensure security and reliability, and extend application longevity.

The State's web development strategy is evolving and is updated periodically to reflect new products and services and to incorporate additional guidelines to protect against newly discovered security threats. Appropriately, this document will be updated to reflect newly discovered information.

Common Look and Feel
The State's web portal, *accessIndiana*, is in the process of standardizing the appearance of all departmental and application-specific sites on the www.IN.gov domain. This standardization process provides a common look and feel for users interacting with State government. All existing and new applications and pages shall follow the guidelines for common look and feel. The guidelines state that a site's homepage must conform to specific appearance standards and secondary pages must maintain a similar look and feel, although some flexibility is allowed. *accessIndiana* provides screen templates and graphics design specifications.

Architecture
Web applications shall be designed with the presentation layer, business logic and data logically separated to increase portability, scalability, re-usability and to support simplicity. This design is commonly referred to as a three (3)-tiered, or n-tiered application development architecture. Please see the *Hosting* section of this document for additional information.

Technology Standards
The State maintains a dynamic listing of current technology standards for consideration in new application and page development. The standards are listed in Appendix 1 of this document and include the categories Central Services Supported [*accessIndiana* / Department of Administration - Division of Information Technology (DoIT)], Emerging, Specialized and/or Agency Specific Usage, Declining, Exit Plan. The selected vendor shall utilize products listed in the Central Services Supported, Emerging or Specialized categories. Use of any product not listed requires ITOC approval and a written waiver to use the product submitted by the agency.

Privacy Policy
All applications and pages shall comply with the *accessIndiana* privacy policy. The privacy policy is listed on the *accessIndiana* web site at www.IN.gov.

Accessibility
All applications and pages developed for the State of Indiana must be compatible with the principles and goals contained in the electronic and information technology accessibility standards adopted by the architectural and transportation barriers compliance board under Section 508 of the federal Rehabilitation Act of 1973 (29 U.S.C. 749d), as amended, and with the State Accessibility guidelines developed pursuant to HEA 1926, Acts of 2001. These guidelines are listed via a link on the www.IN.gov homepage.

Payment Processing
Payment processing shall be consistent for all applications hosted on the State's portal. *accessIndiana* maintains a payment processing system. This system can be an easy bolt-on process to most applications as they are being developed. The *accessIndiana* technical staff will provide the payment processing engine and assist the selected vendor with implementation issues. Any deviation from this requires ITOC approval and a written waiver.

Hosting
The *Architecture* section specifies the logical separation of the presentation, application and database layers. This separation is crucial to the State's hosting strategy. A technical evaluation of each application shall determine the appropriate location for hosting each of the presentation, application and database layers. In all cases the presentation layer for Internet delivered applications is hosted at *accessIndiana*. For extranet applications, the presentation layer is hosted at DoIT or accessIndiana.For Intranet applications, presentation layer hosting can be at DoIT or in the agency. Extranet and intranet hosting decisions will be made during the architectural review and will be dependent on the content of the information being presented to determine the hosting location.

The hosting location of the application and the database layers are determined during the architectural review. The responding vendors can anticipate that the presentation, application and database layers could be hosted on different physical hardware devices at different sites on the State's network backbone.

The responding vendors will also provide any environmental requirements including hardware, software and any special network or bandwidth considerations.

Special considerations may be made for outsourced services in which the web site must be hosted outside the www.IN.gov domain. Although this scenario can be accommodated, it is not a preferred hosting solution, because externally hosted applications do not allow for search ability from the *accessIndiana* website. These cases will be evaluated on a case-by-case basis, and will require ITOC written approval. In such cases, the State retains the right to audit the technical and operational procedures to include data security items such as firewall rules, user access to data and data loss prevention. All other provisions of this document remain applicable (with the exception of the *Architecture*, *Technology Standards*, *Security–LDAP Authentication* and *Payment Processing* sections) if the application is to be hosted outside of the www.IN.gov domain.

Support
If requested and applicable, the responding vendors shall include a plan for ongoing application and page support. The plan shall include information regarding the appropriate technical skill sets and approximate quantity of support required. The plan shall also identify whether application support is to be conducted from within the State's network backbone or from an external source outside of the State's firewall systems

Security – Protocols
HTTP and HTTPS traffic (port 80 and port 443) is allowed through the State's firewall systems. Applications requiring additional ports opened on the State's firewall systems are strongly discouraged. If a specific technical solution requires additional firewall ports opened, presentation of that technical solution must identify the additional firewall port(s) and clearly identify the advantages to the state for taking on such an additional security risk.

Security - Presentation Layer Input Validation
Safeguards must be included in all applications to protect the State's data and technical resources. Presentation layer coding must include (at a minimum) specified user input validation checks to guard against unauthorized access. Appendix 2 provides detail of specific presentation layer input validation guidelines.

Security – LDAP Authentication
The State's direction is to allow users to input the same username and password to access different services. This strengthens the State's goal of providing a common look and feel environment in which users perceive they are interacting with State government as a whole, as opposed to many agencies and departments. To meet this challenge the State is installing a common repository for user authentication information. The repository will be constructed using Lightweight Directory Access Protocol (LDAP) standards. Applications requiring user authentication should be coded to utilize the State-supplied LDAP database. Standards for accessing the state directory of portal users for authentication and access control uses will be made available. The use of a secondary sign-on processes is discouraged. However, if the agencies must create and maintain a secondary sign-on process for their respective applications it will be at their own expense. All agency-specific secondary sign on processes are in addition to, not in lieu of, the LDAP directory sign on process.

Source Code Review
The State retains the right to review application source code prior to implementation and while in production status.

Development, Test and Production Servers, Monitoring and Logging
All web-based applications must be tested in an appropriate environment to ensure compatibility, reliability and reasonable performance under load while operating in the State's production environment. It is anticipated that the sophistication and completeness of the testing environment, tools and procedures will be proportional to the size and complexity of the target system. The test environment configuration, tools and procedures will be presented to the agency and the production hosting organizations for review and approval. Applications in development or test status will not be permitted on production servers. Monitoring and logging procedures must be consistent for all applications on the State's portal. The *accessIndiana* technical staff will assist the selected vendor on issues related to logging and monitoring requirements.

Alternate Presentation Layer Formats
The State's preferred architecture (see *Architecture* section) allows the core business rules of an application to be written once and be ported to multiple presentation layer formats such as a web browser, kiosk and wireless browser. The selected vendor can develop the web browser presentation layer and *accessIndiana* or DoIT can develop various alternate presentation layers (such as kiosk and wireless browser) as required to meet the demand for a given application.

STATE OF INDIANA
Web-Based Computing Guidelines for Prospective Vendors

Appendix 1: Technology Positioning Chart

Category Definitions:

Central Services Supported ("Core") – Accepted; State has technical environment to support

Emerging – Accepted; Future strategy/direction. Support not fully evolved.

Specialized and/or Agency Specific ("Specialized") – Conditionally Accepted; Specific technology required to satisfy unique business processes. Support negotiated on case-by-case basis.

Declining – No new development. Exit plan evolving.

Exit Plan – No new development. Exit plan in place to remove.

Topic	Core	Emerging	Specialized	Declining	Exit Plan
I. Data Management and Movement					
Server DBMS	Oracle, SQL Server, DB2			IMS, IDMS	
Database API					
Internet	JDBC				
Intranet	ODBC	JDBC	DB2 Connect		
Data Interchange		XML	EDI		
II. Development Tools					
Application Development Models	N-tier with HTML Client		N-tier with Java Client	Thick Client N-tier	
Query & Reporting	Crystal Reports		Cognos		
Logical & Physical Data Modeling	ERWIN		PowerDesigner, Oracle Designer		
Object Oriented Analysis & Design		UML			
Source Code Management	CVS				
Testing	Expeditor		Mercury WinRunner, LoadRunner, Test Director, Foglight		

STATE OF INDIANA
Web-Based Computing Guidelines for Prospective Vendors

Topic	Core	Emerging	Specialized	Declining	Exit Plan
II. Development Tools					
Programming					
Thin Client N-tier					
Thin Client	HTML 3.2				
Web Server					
Internet	Apache		IIS		
Intranet	IIS	Apache			
Dynamic Page Server					
Internet	Java Servlets	JSP	ASP,,Cold Fusion	Perl, C	Cold Fusion (For Core)
Intranet	JavaScript, Dynascript	Java Servlets, JSP	ASP,VBScript,Cold Fusion	Perl, C	Cold Fusion (For Core)
Component Integration		Enterprise Java Beans	DCOM		
Transaction Server					
Internet, Intranet		Java Transaction Server (JTS)	Microsoft Transaction Server (MTS),		
Database	Oracle, SQL Server, DB2			IMS, IDMS	
Help Desk	Magic Solutions				
Low-level Integration & Performance Reqs.	C, C++				
Server Shell Scripts	Korn			Perl	
Server Tier	Java				
III. Document Technology					
Document Management	Adobe		MS Word		
IV. Network Based Services					
Web Servers					
Internet	Apache		IIS		
Intranet	IIS		Apache		
Mail Servers	MS Exchange			Groupwise	
Mail Client	Outlook, Netscape				
Mail Transport	SMTP				
Mail API	MAPI				
Directory Access Protocol	LDAP				

Topic	Core	Emerging	Specialized	Declining	Exit Plan
V. Networks					
Protocols	TCP/IP			IPX, SNA	
VI. Platforms - Client					
HTML Design	Front Page, DreamWeaver, Homesite				
VII. Platforms - Server					
Server OS					
Web/Dynamic Page Server					
Internet	Solaris	Linux	Win NT, Win 2000		
Intranet	Solaris	OS/390	Win NT, Win 2000		
Database	OS/390, Solaris, Win NT	Win 2000, Linux			
Middle Tier		Solaris, Linux	Win NT, Win 2000		
VIII. Security					
Firewall					
Internet	PIX	Gauntlet, F1	O/S390 Security Server Firewall		
Secure Communication					
Secure FTP / Telnet	SSH				
Digital Certificates		enTrust, O/S390 Security Server			
Certificate Authority		O/S390 Security Server			
Digital Certificates (Server)					
Digital Certificates (Browsers)					
Digital Certificates (e-mail)					

Appendix 2: Presentation Layer Input Validation Guidelines

General input cleaning

- Check (and limit) the size of user input. Be aware of the dangers of buffer overflows (see below)
- Check for dangerous characters in user input such as [. \ !] , etc.

Security through obscurity

- Security through obscurity is a useful tool, but should not be relied upon to limit an attacker from gaining unauthorized access.
- Do not provide information to a user that is not necessary about your operating environment. Error messages should never contain path names, for example.

Buffer overflows

- An excellent reference on the details of conduction buffer overflow attacks is listed under the references section.
- Always check the size of user input before copying it into a fixed length buffer, or limit the amount of data to be copied to the size of the buffer.
- Never assume that external programs, applications, or libraries perform proper input checking.

File system traversal

- Many vulnerabilities have been discovered that involve directory traversal attacks. To guard against these, input should be checked for suspicious strings, such as "../" or "..\" (depending on the operating system in question).

SQL

- If user input is to be used in SQL queries, the following steps must be taken:
- Escaping: Special characters must be escaped. In particular "(",")","'" and depending on your connectivity method and database "&", "[", and "]". The database and connectivity method used may dictate that other characters need to be escaped. These should be identified and handled appropriately.
    - Text fields should always be quoted to prevent users from entering additional SQL statements.
    - Numeric input, which cannot be quoted, should be checked to insure that it contains only numeric values.
    - Database permissions should be appropriate to the level of access required by the application, and if possible the particular query. If inserts and updates are not performed by the application, it should have only read privileges.
    - Understand special features of the database being used. For example, MS SQL server 6.5 allows for a comment in a statement. The presence of "-- " in the query tells SQL server to ignore the rest of the statement. Such characters or character strings should be checked for in user input.

Java

- System calls should be avoided if possible.
- Input should be checked for shell metacharacters. Try using:

```
s/([\&;\`'\\\|"*?~<>^\(\)\[\]\{\}\$\n\r])/\\$1/g;
```

- Input should be checked for NULL characters as well, and they should be eliminated with `s/\0//g;`
- Java security manager should be configured to only allow access to resources necessary for the functioning of the application.

IIS/ASP

- All IIS based applications should be prepared to run in a fully patched NT/IIS environment, with the latest service packs on hotfixes. This is critical to maintaining server security
- Front Page extensions that are not being used should be disabled on the site.
- ASP developers should protect all code from being viewed by users. ASP include files should have the .asp extension to prevent a user from viewing source by referencing the included file directly.
- ISAPI filters should be avoided when possible. They have been a frequent source of buffer overflows, and should not be used unless necessary.
- Consider using ODBC instead of OLEDB. While slower, details of the data source are not contained in the ASP source, but in the system DSN, making access to this information much more difficult for an attacker to obtain.
- All code should be prepared to run under MDAC 2.5 SP1 or later.
- Don't use Remote Data Services (RDS).

References

Perl Security http://www.perl.com/pub/doc/manual/html/pod/perlsec.html
Securityfocus.com - http://www.securityfocus.com/
"Perl CGI problems" by rain.forest.puppy
http://www.phrack.com/search.phtml?view&article=p55-7
"Smashing The Stack For Fun And Profit" by Aleph One
http://www.phrack.com/search.phtml?view&article=p49-14
"NT Web Technology Vulnerabilities" by rain.forest.puppy
http://www.phrack.com/search.phtml?view&article=p54-8